УДК 004.056

МНОГОУРОВНЕВОЕ ШИФРОВАНИЕ С ИЕРАРХИЕЙ КЛЮЧЕЙ

Студент гр. 113026 Е.В. Гнутенко,
преподаватель И.Л. Алифанова, ст. преподаватель О.В. Дубровина

Белорусский национальный технический университет

Целью данного проекта является реализация схемы "цифрового конверта" с использованием эллиптических кривых. Конфиденциальная информация шифруется симметричным алгоритмом, что позволяет надежно и быстро обрабатывать значительные объемы данных. Ключ, используемый при этом, скрывается асимметричным алгоритмом. В результате обеспечивается решение сразу нескольких задач: аутентификация пользователя подтверждается при верификации симметричного ключа; протокол обмена ключами не требует аутентичного канала связи и может использовать открытые сети. Иерархия ключей обеспечивает безопасность скрываемой информации и секретность ключа собственно шифрования.

В качестве базовых алгоритмов были выбраны самые последние международные стандарты: для симметричного шифрования реализован алгоритм Rijndael (реализован в базовом варианте), асимметричный алгоритм базируется на эллиптических кривых, схема основана на сложной задаче нахождения точки на эллиптической кривой. Rijndael реализован в базовом варианте. Длина ключа 256 бит и структура математических преобразований алгоритма обеспечивают высокий уровень надежности шифрования. Асимметричная задача использует конечное простое поле, представляемое как множество из p целых чисел {0, 1, ..., p-1}, где p = 2256, из которого происходит выборка значений для получения кривой. Каждая сгенерированная кривая проходит проверку на сингулярность, чтобы убедиться в ее криптографической стойкости.

Основной функционал предлагаемого приложения обладает следующими возможностями:

1) Шифрование\дешифрование файлов и папок симметричным алгоритмом AES. При шифровании папок возможно применение алгоритмов сжатия, используются форматы MsZip, Lzx. При помощи персональных настроек исходные файлы и папки, использовавшиеся для шифрования или дешифровки, могут быть удалены.
2) Сокрытие ключа, использованного на предыдущем шаге, ассиметричным алгоритмом на базе эллиптических кривых. Все публичные значения, полученные в ходе работы программы, могут быть сохранены в файл или загружены из файла. Возможно сохранение в файл и загрузка из файла значений, связанных непосредственно с параметрами кривой.

3) Создание, монтирование и отсоединение безопасного диска. Файлы, помещенные на монтированный диск, автоматически шифруются новым сеансовым ключом (а сам ключ – эллиптическими кривыми) при отсоединении виртуального устройства.
4) Все поля, в которые вводится секретный ключ пользователя, защищены от "клавиатурных шпионов".
5) Ассоциация программы с создаваемыми ею файлами.
6) Возможность изменение стиля оформления программы.
7) Возможность автоматического обновления версий программы через сеть Интернет.

Нетривиальной опцией программы является "безопасный диск" (Secure drive). Приложение по запросу пользователя создает виртуальный жесткий диск. Виртуальное устройство представляет собой файл-образ будущего безопасного диска, после монтировки которого он будет доступен как обычный локальный диск из любого файлового менеджера. Можно перемещать на него все файлы, требующие обеспечения безопасности, производить необходимые действия с содержимым диска, и отмонтировать его, в результате чего все данные, находящиеся на диске, будут зашифрованы.

Еще одна немаловажная опция, усиливающая безопасность приложения – защита от клавиатурных шпионов. Все поля, в которые вводятся секретный пароль пользователя, защищены по одному принципу: компонент ввода посылает ОС бесконечное множество сообщений со случайными комбинациями. Этот процесс фактически не влияет на быстродействие приложения, но делает невозможным считывание приватной информации.

Интересной возможностью является также возможность проассоциировать приложение с основными типами файлов, используемых им. Ассоциация позволяет не только сообщить системе о типе файлов и родительском приложении, но и организовать взаимодействие этих файлов с программой. Приложение имеет дружественный интерфейс и возможность персональных настроек. Все опции и значения программы сохраняются в файл настроек.

Программа содержит специальный модуль, срабатывающий в случае, когда графический интерфейс программы не отвечает, например, при шифровании большого объема информации. Пользователю посылается немодальное окно с сообщением о занятости приложения и просьбой обождать.

Приложение обладает возможностью автоматического обновления из сети Интернет. Процесс обновления полностью автоматизирован, пользователю стоит лишь выбрать соответствующий пункт в главном меню программы и следовать указаниям менеджера обновления.